IN THE SPECIFICATION

Please amend the paragraphs beginning at page 5, line 24 as follows:

To accomplish the above object, <u>Applicants disclose an</u> ~~a first~~ IP communication network system<u>, apparatus and method according to the present invention. The IP communication network system comprises</u> ~~according to the present invention comprising~~ a plurality of autonomous systems, configuring IP networks of domains independent of each other, for performing interior- and exterior-forwarding of IP packets. The plurality of autonomous systems include a plurality of border relay devices positioned at borders between the IP networks. Each of the plurality of border relay devices includes a discarding unit for discarding, if the IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet, and a distribution unit for distributing the filtering information to all other border relay devices within the same autonomous system.

~~In a second IP communication network system according to the present invention, a~~ <u>A</u> host computer of each of the plurality of autonomous systems includes a detection unit for detecting based on predetermined items of judging information that the IP packet forwarded is the unauthorized intrusion packet. <u>Once detected,</u> ~~In a third IP communication network system according to the present invention~~, the distribution unit of the border relay device further distributes the filtering information to the border relay device within the autonomous system facing to the autonomous system from which the unauthorized packet is forwarded.

~~In a fourth IP communication network system according to the present invention, each of a plurality of relay devices positioned at relay points between the respective IP networks of the plurality of autonomous systems~~ <u>A border relay device in the autonomous system</u> includes a

2

discarding unit for discarding, if the IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet; and a distribution unit for distributing the filtering information to all the relay devices within the same autonomous system.

A first border relay device according to the present invention, is positioned at a border between autonomous systems, configuring IP networks of independent domains, for performing interior- and exterior- forwarding of an IP packet. The border relay device comprises a discarding unit for discarding, if the IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet, and a distribution unit for distributing the filtering information to all other border relay devices within the autonomous systems.

In a second border relay device according to the present invention, the distribution unit further distributes the filtering information to the border relay device positioned at a border within the autonomous system facing to the autonomous system from which the unauthorized packet is forwarded.

A first unauthorized intrusion safeguard method according to the present invention in an IP communication network system having a plurality of autonomous systems, configuring IP networks of independent domains of each other, for performing interior- and exterior-forwarding of IP packets, the method in each of the plurality of autonomous systems, comprises a step of detecting that the IP packet forwarded is an unauthorized intrusion packet on the basis of predetermined items of judging information, a step of discarding the unauthorized packet at one border of the IP network when detecting a re-intrusion on the basis of filtering information for

3

detecting the re-intrusion of the unauthorized packet, and a step of distributing the filtering information to all other border relay devices within the same autonomous system.

A second unauthorized intrusion safeguard method according to the present invention may further comprise a step of distributing the filtering information to the border within the autonomous system facing to the autonomous system from which the unauthorized packet is forwarded.

A third unauthorized intrusion safeguard method according to the present invention may further, in each of the plurality of autonomous systems, comprise a step of discarding, when the IP packet forwarded is an unauthorized intrusion packet, the unauthorized packet at one border of the IP network when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet, and a step of distributing the filtering information to all other relay points within the same autonomous system.

A fourth authorized intrusion safeguard method according to the present invention comprises a step of discarding, if an IP packet forwarded is an unauthorized intrusion packet, this unauthorized packet when detecting a re-intrusion on the basis of filtering information for detecting the re-intrusion of the unauthorized packet at a border between autonomous systems, configuring IP networks of independent domains, for performing interior- and exterior-forwarding of the IP packet, and a step of distributing the filtering information to all other borders within the autonomous systems.

A fifth authorized intrusion safeguard method according to the present invention may further comprise a step of distributing the filtering information to a border within the autonomous system facing to the autonomous system from which the unauthorized packet is forwarded.

4